

ISSA

Fundamentals of Information Systems Security

THIRD EDITION

David Kim | Michael G. Solomon



JONES & BARTLETT
LEARNING

Contents

Preface	xix
Acknowledgments	xxi
The Authors	xxi

PART I

The Need for Information Security 1

CHAPTER 1

Information Systems Security 2

Information Systems Security 3

Risks, Threats, and Vulnerabilities	11
What Is Information Systems Security?	12
U.S. Compliance Laws Drive Need for Information Systems Security	12

Tenets of Information Systems Security 14

Confidentiality	16
Integrity	17
Availability	17

The Seven Domains of a Typical IT Infrastructure 19

User Domain	19
Workstation Domain	22
LAN Domain	22
LAN-to-WAN Domain	25
WAN Domain	28
Remote Access Domain	32
System/Application Domain	36

Weakest Link in the Security of an IT Infrastructure 38

Ethics and the Internet	40
-------------------------	----

IT Security Policy Framework 40

Definitions	41
Foundational IT Security Policies	41

Data Classification Standards 42

CHAPTER SUMMARY 44

KEY CONCEPTS AND TERMS 44

CHAPTER 1 ASSESSMENT 45

CHAPTER 2**The Internet of Things Is Changing How We Live 47****Evolution of the Internet of Things 49****Converting to a TCP/IP World 50****IoT's Impact on Human and Business Life 51**

How People Like to Communicate 52

IoT Applications That Impact Our Lives 52

Evolution from Bricks and Mortar to E-Commerce 55**Why Businesses Must Have an Internet
and IoT Marketing Strategy 57****IP Mobility 58**

Mobile Users and Bring Your Own Device 58

Mobile Applications 59

IP Mobile Communications 60

New Challenges Created by the IoT 62

Security 62

Privacy 63

Interoperability and Standards 65

Legal and Regulatory Issues 67

E-Commerce and Economic Development Issues 68

CHAPTER SUMMARY 69**KEY CONCEPTS AND TERMS 70****CHAPTER 2 ASSESSMENT 70****CHAPTER 3****Malicious Attacks, Threats, and Vulnerabilities 72****Malicious Activity on the Rise 73****What Are You Trying to Protect? 74**

Customer Data 74

IT and Network Infrastructure 75

Intellectual Property 76

Finances and Financial Data 76

Service Availability and Productivity 77

Reputation 78

Whom Are You Trying to Catch? 78**Attack Tools 79**

Protocol Analyzers 80

Port Scanners 80

OS Fingerprint Scanners 80

Vulnerability Scanners 80

Exploit Software 81

Wardialers 81

Password Crackers	82
Keystroke Loggers	82
What Is a Security Breach?	83
Denial of Service Attacks	83
Distributed Denial of Service Attacks	84
Unacceptable Web Browsing	84
Wiretapping	85
Backdoors	85
Data Modifications	86
Additional Security Challenges	86
What Are Risks, Threats, and Vulnerabilities?	88
Threat Targets	89
Threat Types	90
What Is a Malicious Attack?	92
Birthday Attacks	93
Brute-Force Password Attacks	93
Dictionary Password Attacks	94
IP Address Spoofing	94
Hijacking	94
Replay Attacks	95
Man-in-the-Middle Attacks	95
Masquerading	96
Eavesdropping	96
Social Engineering	96
Phreaking	97
Phishing	97
Pharming	98
What Is Malicious Software?	99
Viruses	99
Worms	100
Trojan Horses	100
Rootkits	101
Spyware	101
What Are Common Types of Attacks?	102
Social Engineering Attacks	103
Wireless Network Attacks	104
Web Application Attacks	104
What Is a Countermeasure?	106
Countering Malware	106
Protecting Your System with Firewalls	108
CHAPTER SUMMARY	108
KEY CONCEPTS AND TERMS	109
CHAPTER 3 ASSESSMENT	110

CHAPTER 4	The Drivers of the Information Security Business	112
	Defining Risk Management	113
	Implementing a BIA, a BCP, and a DRP	115
	Business Impact Analysis	115
	Business Continuity Plan	116
	Disaster Recovery Plan	118
	Assessing Risks, Threats, and Vulnerabilities	122
	Closing the Information Security Gap	123
	Adhering to Compliance Laws	124
	Keeping Private Data Confidential	127
	Mobile Workers and Use of Personally Owned Devices	129
	BYOD Concerns	129
	Endpoint and Device Security	130
	CHAPTER SUMMARY	131
	KEY CONCEPTS AND TERMS	132
	CHAPTER 4 ASSESSMENT	132
PART II	Securing Today's Information Systems	135
CHAPTER 5	Access Controls	136
	Four-Part Access Control	137
	Two Types of Access Controls	138
	Physical Access Control	138
	Logical Access Control	138
	Authorization Policies	140
	Methods and Guidelines for Identification	141
	Identification Methods	141
	Identification Guidelines	141
	Processes and Requirements for Authentication	142
	Authentication Types	142
	Single Sign-On	151
	Policies and Procedures for Accountability	154
	Log Files	154
	Monitoring and Reviews	154
	Data Retention, Media Disposal, and Compliance Requirements	154
	Formal Models of Access Control	156
	Discretionary Access Control	157
	Operating Systems-Based DAC	157

Mandatory Access Control	159
Nondiscretionary Access Control	160
Rule-Based Access Control	160
Access Control Lists	160
Role-Based Access Control	161
Content-Dependent Access Control	163
Constrained User Interface	163
Other Access Control Models	164
Effects of Breaches in Access Control	166
Threats to Access Controls	167
Effects of Access Control Violations	168
Credential and Permissions Management	169
Centralized and Decentralized Access Control	169
Types of AAA Servers	169
Decentralized Access Control	172
Privacy	172
CHAPTER SUMMARY	177
KEY CONCEPTS AND TERMS	177
CHAPTER 5 ASSESSMENT	178

CHAPTER 6

Security Operations and Administration	181
Security Administration	182
Controlling Access	182
Documentation, Procedures, and Guidelines	183
Disaster Assessment and Recovery	183
Security Outsourcing	184
Compliance	185
Event Logs	186
Compliance Liaison	186
Remediation	186
Professional Ethics	187
Common Fallacies About Ethics	187
Codes of Ethics	188
Personnel Security Principles	189
The Infrastructure for an IT Security Policy	192
Policies	192
Standards	194
Procedures	194
Baselines	195
Guidelines	196

Data Classification Standards	196
Information Classification Objectives	197
Examples of Classification	197
Classification Procedures	197
Assurance	198
Configuration Management	199
Hardware Inventory and Configuration Chart	199
The Change Management Process	200
Change Control Management	200
Change Control Committees	201
Change Control Procedures	202
Change Control Issues	203
Application Software Security	203
The System Life Cycle	203
Testing Application Software	205
Software Development and Security	208
Software Development Models	209
CHAPTER SUMMARY	212
KEY CONCEPTS AND TERMS	213
CHAPTER 6 ASSESSMENT	213
Auditing, Testing, and Monitoring	216
Security Auditing and Analysis	217
Security Controls Address Risk	218
Determining What Is Acceptable	219
Permission Levels	219
Areas of Security Audits	220
Purpose of Audits	220
Customer Confidence	221
Defining Your Audit Plan	223
Defining the Scope of the Plan	223
Auditing Benchmarks	224
Audit Data Collection Methods	226
Areas of Security Audits	226
Control Checks and Identity Management	227
Post-Audit Activities	228
Exit Interview	228
Data Analysis	228
Generation of Audit Report	228
Presentation of Findings	229

CHAPTER 7

Security Monitoring	229
Security Monitoring for Computer Systems	230
Monitoring Issues	231
Logging Anomalies	232
Log Management	232
Types of Log Information to Capture	233
How to Verify Security Controls	234
Intrusion Detection System (IDS)	234
Analysis Methods	236
HIDS	237
Layered Defense: Network Access Control	237
Control Checks: Intrusion Detection	238
Host Isolation	238
System Hardening	238
Review Antivirus Programs	241
Monitoring and Testing Security Systems	241
Monitoring	241
Testing	241
CHAPTER SUMMARY	249
KEY CONCEPTS AND TERMS	249
CHAPTER 7 ASSESSMENT	249

CHAPTER 8

Risk, Response, and Recovery	251
Risk Management and Information Security	252
Risk Terminology	253
Elements of Risk	254
Purpose of Risk Management	254
The Risk Management Process	255
Identify Risks	256
Assess Risks	259
Plan a Risk Response	263
Implement the Risk Response Plan	265
Monitor and Control Risk Response	269
Business Continuity Management	270
Terminology	271
Assessing Maximum Tolerable Downtime	272
Business Impact Analysis	273
Plan Review	274
Testing the Plan	274
Backing Up Data and Applications	276
Types of Backups	276

Incident Handling 277

Preparation	278
Identification	278
Notification	278
Response	279
Recovery	280
Followup	280
Documentation and Reporting	280

Recovery from a Disaster 280

Activating the Disaster Recovery Plan	281
Operating in a Reduced/Modified Environment	281
Restoring Damaged Systems	282
Disaster Recovery Issues	282
Recovery Alternatives	282
Interim or Alternate Processing Strategies	283

CHAPTER SUMMARY 285**KEY CONCEPTS AND TERMS 286****CHAPTER 8 ASSESSMENT 287****CHAPTER 9****Cryptography 288****What Is Cryptography? 289**

Basic Cryptographic Principles	290
A Brief History of Cryptography	291
Cryptography's Role in Information Security	292

Business and Security Requirements for Cryptography 295

Internal Security	295
Security in Business Relationships	295
Security Measures That Benefit Everyone	296

Cryptographic Principles, Concepts, and Terminology 296

Cryptographic Functions and Ciphers	296
-------------------------------------	-----

Types of Ciphers 299

Transposition Ciphers	300
Substitution Ciphers	300
Product and Exponentiation Ciphers	302

Symmetric and Asymmetric Key Cryptography 303

Symmetric Key Ciphers	303
Asymmetric Key Ciphers	304
Cryptanalysis and Public Versus Private Keys	305

Keys, Keyspace, and Key Management 308

Cryptographic Keys and Keyspace	308
Key Management	309
Key Distribution	310
Key Distribution Centers	310

Digital Signatures and Hash Functions	311
Hash Functions	311
Digital Signatures	311
Cryptographic Applications and Uses in Information System Security	312
Other Cryptographic Tools and Resources	313
Symmetric Key Standards	314
Asymmetric Key Solutions	316
Hash Function and Integrity	318
Digital Signatures and Nonrepudiation	320
Principles of Certificates and Key Management	321
Modern Key Management Techniques	321
CHAPTER SUMMARY	323
KEY CONCEPTS AND TERMS	324
CHAPTER 9 ASSESSMENT	324

CHAPTER 10

Networks and Telecommunications	326
The Open Systems Interconnection Reference Model	327
The Main Types of Networks	329
Wide Area Networks	329
Local Area Networks	332
TCP/IP and How It Works	334
TCP/IP Overview	334
IP Addressing	335
Common Ports	336
Common Protocols	336
Internet Control Message Protocol	336
Network Security Risks	338
Categories of Risk	338
Basic Network Security Defense Tools	341
Firewalls	341
Virtual Private Networks and Remote Access	345
Network Access Control	347
Wireless Networks	347
Wireless Access Points	348
Wireless Network Security Controls	348
CHAPTER SUMMARY	351
KEY CONCEPTS AND TERMS	351
CHAPTER 10 ASSESSMENT	352

CHAPTER 11

Malicious Code and Activity 354**Characteristics, Architecture,
and Operations of Malicious Software 355****The Main Types of Malware 356**

Virus	356
Spam	363
Worms	364
Trojan Horses	366
Logic Bombs	367
Active Content Vulnerabilities	367
Malicious Add-Ons	367
Injection	368
Botnets	369
Denial of Service Attacks	369
Spyware	371
Adware	372
Phishing	372
Keystroke Loggers	373
Hoaxes and Myths	373
Homepage Hijacking	374
Webpage Defacements	374

A Brief History of Malicious Code Threats 375

1970s and Early 1980s: Academic Research and UNIX	375
1980s: Early PC Viruses	376
1990s: Early LAN Viruses	376
Mid-1990s: Smart Applications and the Internet	377
2000 to Present	377

Threats to Business Organizations 378

Types of Threats	378
Internal Threats from Employees	379

Anatomy of an Attack 379

What Motivates Attackers?	380
The Purpose of an Attack	380
Types of Attacks	380
Phases of an Attack	382

Attack Prevention Tools and Techniques 387

Application Defenses	388
Operating System Defenses	388
Network Infrastructure Defenses	389
Safe Recovery Techniques and Practices	390
Implementing Effective Software Best Practices	390

Intrusion Detection Tools and Techniques 390

Antivirus Scanning Software	391
Network Monitors and Analyzers	391

Content/Context Filtering and Logging Software	391
Honeypots and Honeynets	392

CHAPTER SUMMARY 393

KEY CONCEPTS AND TERMS 393

CHAPTER 11 ASSESSMENT 393

PART III Information Security Standards, Education, Certifications, and Laws 395

CHAPTER 12

Information Security Standards 396

Standards Organizations 397

National Institute of Standards and Technology	397
International Organization for Standardization	398
International Electrotechnical Commission	400
World Wide Web Consortium	401
Internet Engineering Task Force	401
Institute of Electrical and Electronics Engineers	403
International Telecommunication Union Telecommunication Sector	404
American National Standards Institute	405
European Telecommunications Standards Institute	
Cyber Security Technical Committee	406

ISO 17799 (Withdrawn) 407

ISO/IEC 27002	408
---------------	-----

Payment Card Industry Data Security Standard 409

CHAPTER SUMMARY 410

KEY CONCEPTS AND TERMS 411

CHAPTER 12 ASSESSMENT 411

CHAPTER 13

Information Systems Security Education and Training 412

Self-Study Programs 413

Instructor-Led Programs 416

Certificate Programs	416
Continuing Education Programs	418

Postsecondary Degree Programs 419

Associate's Degree	420
Bachelor's Degree	420
Master of Science Degree	421
Master of Business Administration	423
Doctoral Degree	424

Information Security Training Programs 425

Security Training Requirements	426
Security Training Organizations	427
Security Awareness Training	428

CHAPTER SUMMARY 430**KEY CONCEPTS AND TERMS 430****CHAPTER 13 ASSESSMENT 431****CHAPTER 14****Information Security Professional Certifications 433****U.S. Department of Defense/Military Directive 8570.01 434**

U.S. DoD/Military Directive 8140	434
U.S. DoD/NSA Training Standards	436

Vendor-Neutral Professional Certifications 437

International Information Systems Security Certification Consortium, Inc.	438
SSCP®	438
CISSP®	438
CAP®	439
CSSLP®	439
CCFP®	439
HCISPP®	439
CCSP®	440

Additional (ISC)² Professional Certifications 440

Global Information Assurance Certification/SANS Institute 440

Certified Internet Webmaster 441

CompTIA 441

ISACA® 443

Other Information Systems Security Certifications 443

Vendor-Specific Professional Certifications 443

Cisco Systems 444

Juniper Networks 447

RSA 447

Symantec 447

Check Point 449

CHAPTER SUMMARY 449**KEY CONCEPTS AND TERMS 450****CHAPTER 14 ASSESSMENT 450****CHAPTER 15****U.S. Compliance Laws 452****Compliance Is the Law 453****Federal Information Security 456**

The Federal Information Security Management Act of 2002 456

The Federal Information Security Modernization Act of 2014 458

The Role of the National Institute of Standards and Technology	459
National Security Systems	461
The Health Insurance Portability and Accountability Act	461
Purpose and Scope	461
Main Requirements of the HIPAA Privacy Rule	462
Main Requirements of the HIPAA Security Rule	464
Oversight	464
Omnibus Regulations	466
The Gramm-Leach-Bliley Act	467
Purpose and Scope	469
Main Requirements of the GLBA Privacy Rule	470
Main Requirements of the GLBA Safeguards Rule	471
Oversight	472
The Sarbanes-Oxley Act	472
Purpose and Scope	473
SOX Control Certification Requirements	473
SOX Records Retention Requirements	475
Oversight	475
The Family Educational Rights and Privacy Act	476
Purpose and Scope	476
Main Requirements	477
Oversight	478
The Children's Internet Protection Act	478
Purpose and Scope	478
Main Requirements	479
Oversight	480
Payment Card Industry Data Security Standard	480
Purpose and Scope	481
Self-Assessment Questionnaire	481
Main Requirements	482
Making Sense of Laws for Information Security Compliance	486
CHAPTER SUMMARY	487
KEY CONCEPTS AND TERMS	488
CHAPTER 15 ASSESSMENT	488
ENDNOTES	489

APPENDIX A	Answer Key	491
APPENDIX B	Standard Acronyms	493
APPENDIX C	Earning the CompTIA Security+ Certification	495
	Glossary of Key Terms	498
	References	522
	Index	527